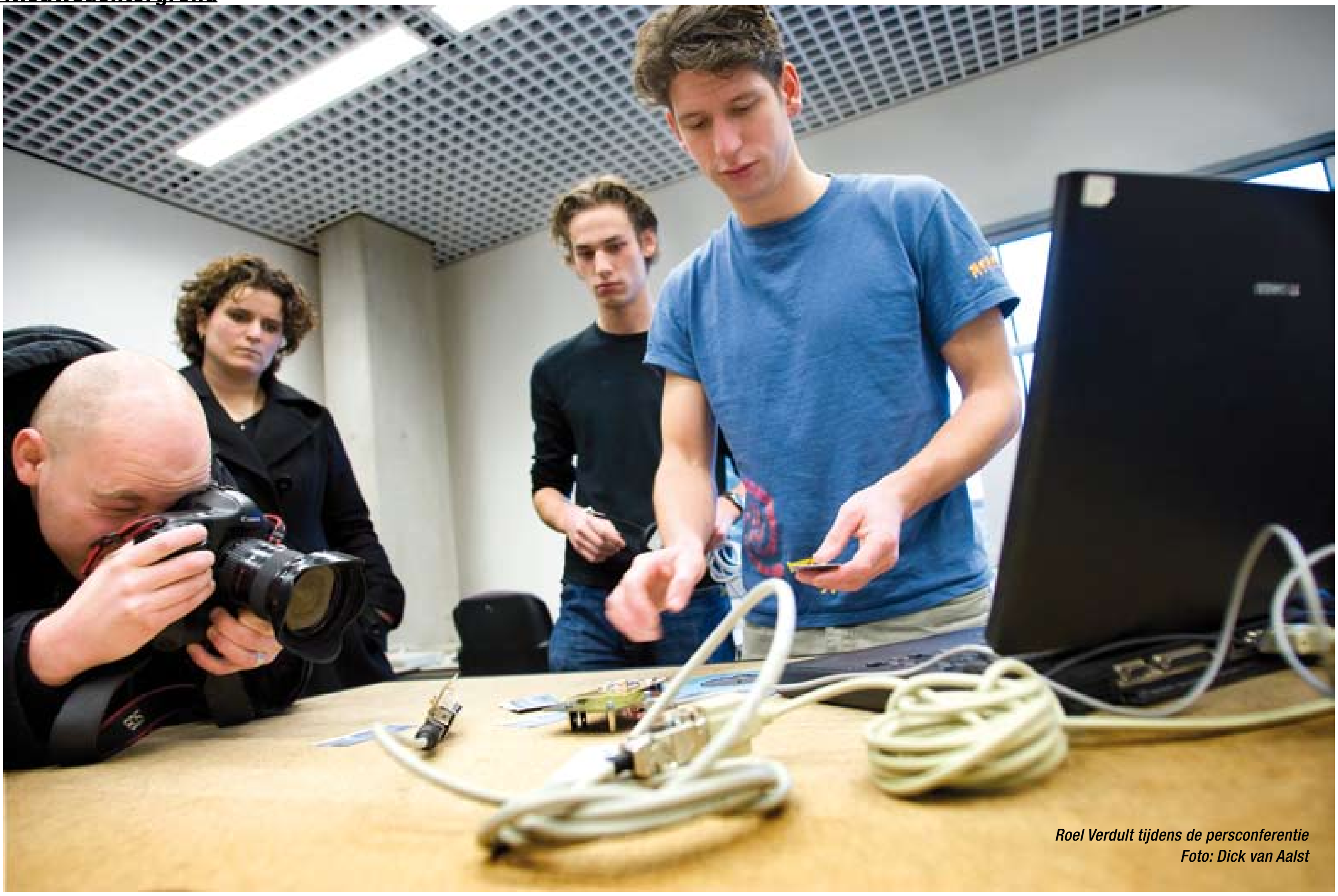


Roel Verdult tijdens de persconferentie
Foto: Dick van Aalst

Reconstructie van **een chipkraak**

Op maandag 14 januari en dinsdag 15 januari beheerst Nijmeegs onderzoek de media. Roel Verdult, student informatica, kraakt de chip in de wegwerpkaartjes voor het OV. Een reconstructie over de rol van de Duitsers, een misgelopen scoop en een bezoek aan de staatssecretaris.

Het is januari 2007 wanneer Roel Verdult, nu 25 jaar oud, aan het werk gaat bij de vakgroep Security of Systems. Zijn afstudeeronderwerp is RFID, dat staat voor Radio Frequency Identification. Via die technologie kan er op afstand informatie worden gelezen en verwerkt. Informatie op een chip bijvoorbeeld die is verwerkt in een stuk papier, of in een pasje om de deur mee te openen. Binnen Security Of Systems wordt dergelijke technologie kritisch gevolgd. De groep onder leiding van Bart Jacobs, hoogleraar computerbeveiliging, onderzoekt hoe veilig internetbankieren, pasjes en betaalsystemen zijn. Daarbij speelt de bewaking van privacygegevens ook een grote rol. Onderzoeksonderwerpen ontstaan vaak aan de koffietafel, vertelt Bart Jacobs. “Tijdens de lunch wordt er geregeld gediscussieerd over de nieuwste ontwikkelingen.” De nieuw in te voeren OV-chipkaart is een dankbaar onderwerp voor discussie. Producent Trans Link Systems uit Amersfoort doet uiterst geheimzinnig over de kaarten. Het betreft een miljoenenproject, maar niemand weet precies hoe het systeem gaat werken en hoe veilig het is. Wanneer de onderzoekers er achter komen dat voor de wegwerpkaartjes de goedkope Mifare Ultralight Chip is gebruikt, weten ze dat de mogelijkheid er is deze te kraken. “Dat is geen arrogantie,” aldus postdoc Wouter Teepe. “Maar het is hier de normaalste zaak van de wereld om dingetjes te kraken. En naar dit systeem gaan zo veel mensen kritisch kijken dat het gewoon een kwestie van tijd is voordat er een lek in wordt gevonden.” Maar het duurt nog even voor ze op dat punt zijn.

Ghost

De eerste vier maanden van zijn onderzoek werkt Verdult aan het apparaat, dat de onderzoekers uiteindelijk de naam Ghost geven. De Ghost is een soort spion in de vorm van een platte kaart die de communicatie tussen het wegwerpkaartje en de lezer kan opvangen, kopiëren en nabootsen. De Ghost kan ook de infor-

matie veranderen waardoor er onbeperkt gereisd kan worden. Tussen mei en september is de software aan de beurt.
Verdult: "Daarna kwam de periode van testen en het zoeken van een case om de Ghost mee te gebruiken." Die eerste case wordt het parkeersysteem van het Huygensgebouw. De parkeerkaartjes zijn een makkelijke prooi voor Ghost. De chip in de OV-kaartjes kost wat meer moeite. Op 14 november reist Verdult met medestudent Gerhard de Koning Gans naar Rotterdam. Het vervoersbedrijf RET gebruikt daar de wegwerpkaartjes met een chip. Verdult en De Koning Gans doen een eerste test die de nodige informatie oplevert.
Bang om betrapt te worden zijn ze niet, ze reizen immers ook beide op een OV studentenkaart. Verdult: "De Ghost kun je makkelijk in je mouw steken en dat hebben we ook gedaan. Maar in Rotterdam bleken de echte wegwerpkaartjes zelfs niet te werken, er stonden veel passagiers te vloeken bij de poortjes. Het was dus niet eens opgevallen als de Ghost niet had gewerkt. Het was natuurlijk wel raar dat wij de hele tijd de poortjes in en uit liepen, maar niemand lette op ons." Verdult wist in Nijmegen al dat het systeem in theorie moest werken. "Maar iedere programmeur weet dat het in de praktijk anders kan uitpakken, daarom was ik ook verbaasd dat de Ghost in een keer goed bleek te werken. Zelfs beter nog dan de echte wegwerpkaartjes."
Rond die tijd hoort ook hoogleraar Bart Jacobs hoe ver het onderzoek is gevorderd. "Ik heb toen gelijk met Roel overlegd en gezegd dat dit heel groot zou worden wanneer het naar buiten komt. Omdat er zo veel geld en zoveel belangen zijn gemoeid met dit systeem, wist ik dat het een politiek gevoelig onderwerp is. Maar ik vond dat het niet een negatief verhaal mocht worden. Hadden we het toen naar buiten gebracht dan was het 'student kraakt kaart' geworden en niets meer dan dat. Het moest duidelijk zijn dat dit ingebed lag in een breder onderzoek naar informatiebeveiliging en privacy, zodat er een genuanceerd beeld naar buiten kon worden gebracht. We hebben toen besloten dat Roel eerst zijn scriptie zou afmaken voordat we het nieuws bekend maakten." De volgende twee maanden werkt Verdult aan zijn scriptie over het onderwerp.

Cameraploeg
Tijdens de laatste dagen van december maakt de Duitse onderzoeker Karsten Nohl tijdens het Chaos Communication Congress bekend hoe hij samen met Henryk Plötz met een microscoop en wat poeder heeft ontcijferd hoe de Mifare Classic chip werkt. Deze duurdere chip gaat gebruikt worden voor de OV-chipkaart, de nieuwe betaalpas voor het OV. Via zogenaamde reverse engineering weten de Duitsers, die op de universiteit van Virginia werkzaam zijn, hoe de beveiliging werkt. Ze weten echter nog niet hoe ze die kunnen kraken.
Op vrijdag 4 januari wordt het nieuws van de Duitsers in Nederland opgepikt, een cameraploeg van *RTL Nieuws* reist op dinsdag 8 januari naar Nijmegen om Bart Jacobs te ondervragen over het onderzoek van de Duitsers. De journalisten informeren tussen neus en lippen ook nog even of er in Nijmegen een onderzoek loopt naar de OV-chipkaarten, maar Jacobs wil de resultaten van het Nijmeegse onderzoek op dat moment nog niet prijsgeven.
Een dag later, woensdag 9 januari, overlegt Jacobs met Verdult. "We hebben toen besloten dat we naar buiten moesten komen met het verhaal. Nu de Duitsers al zo ver waren met die andere chip zou het mensen op ideeën kunnen brengen om de chips van de wegwerpkaartjes te gaan testen. De volgende dag belde Koen de Regt, de reporter van *RTL Nieuws*, me weer omdat hij toch echt wilde weten hoe het zat met ons onderzoek naar de chips in de wegwerpkaartjes. Toen besloot ik om *RTL* de scoop te geven."
Zaterdag, 12 januari, reist Verdult met medestudent Ruben Muijrers weer naar Rotterdam voor een laatste test op het station. Ghost blijkt nu perfect te werken, na het kopen van één wegwerpkaartje kunnen ze in theorie ongelimiteerd de poortjes passeren en dus ook reizen. "We hebben het gehele scenario wat we op *RTL* wilden laten zien meerdere malen getest."
Jacobs: "Dat weekend vertrok ik naar het buitenland voor een reis die al lang gepland stond. Maar ik voelde aan dat er een flink circus los zou barsten na de uitzending maandag. Ik heb dat ook tegen Roel gezegd en gevraagd of hij er klaar voor was om twee weken in de belangstelling te staan. Roel gaf aan dat hij het aandurfde en met postdoc Wouter Teepe heb ik afgesproken dat hij de perscontacten zou afhandelen."
Op maandag 14 januari worden de opnames gemaakt voor het *RTL Nieuws* in Rotterdam.
Het *RTL Nieuws* pakt flink uit met de reportage. Het is de opening en ze ruimen er vijf minuten voor in, uitzonderlijk lang voor een nieuwsitem op televisie.
Diezelfde dag wordt producent Trans Link Systems geïnformeerd, die geschokt reageren. Volgens Wouter Teepe is TLS "not amused, maar desondanks hoffelijk. "We zijn natuurlijk toch de kwajongens die kijken of je iets stuk kunt maken, maar we gaan er wel op een verantwoorde manier mee om. Je moet in dit soort zaken toch een beetje pragmatisch te werk gaan."

'We zijn natuurlijk toch de kwajongens die kijken of je iets stuk kunt maken'

TLS heeft voor de volgende dag dan al een persconferentie belegd. Woordvoerder Jannemieke Zandee: "Vanwege het nieuws van de Duitsers wilden we meer uitleg geven over de veiligheid en de privacy van de OV-chipkaart. Toen het nieuws uit Nijmegen kwam, was het vooral zaak om uit te leggen dat er een verschil is tussen de wegwerpkaartjes en de duurdere OV-chipkaart. Veel media, maar ook politici gooien alles op een hoop. Dat dit nieuws vlak na de onthulling van de Duitsers kwam, maakte het voor ons heel moeilijk om uit te leggen dat er een verschil zit tussen de wegwerpkaartjes en de OV-chipkaart. Voor de wegwerpkaartjes gold een ingecalculeerd en afgewogen risico. De kaartjes worden ook door een beperkt aantal vervoersbedrijven gebruikt en voor speciale evenementen. We zijn nu uiteraard bezig om het systeem veiliger te maken. Hoe we dat doen, vertel ik niet."

Kamerdebat
De technici van TLS komen op dinsdag 15 januari naar Nijmegen om zich door Verdult en Teepe te laten informeren over de kraak van de chip. Verdult: "Ik was op zich niet bang voor de confrontatie met TLS, maar het was wel fijn dat ik niet in m'n eentje tegenover de drie mensen van TLS zat." 's Avonds zit Teepe in *NOVA*. De volgende dag gaan Teepe en Verdult naar Den Haag om in een hoorzitting de kamerleden te informeren. Verdult: "Het ene kamerlid was goed op de hoogte, een ander wist nog van niks. Maar ik heb het idee dat ze de informatie allemaal goed hebben begrepen, dat bleek ook wel in het debat de volgende dag." Vlak voor dat debat moeten Teepe en Verdult bij staatssecretaris Tineke Huizinga langs om over hun bevindingen te vertellen. Wouter Teepe: "Het is spannend om bij *NOVA* en *RTL Nieuws* te zitten, maar de vraag blijft staan wat je bijdraagt. Dat de politiek het oppikt is voor ons het bewijs dat er erkenning komt voor het onderliggende idee waarmee we hier werken. Dat gaf echt het gevoel dat we serieus werden genomen."

Voor de onderzoekers en de politici is het nu wachten tot de Duitsers Karsten Nohl en Henryk Plötz met hun bevindingen naar buiten komen. Dan zal blijken of de duurdere chip ook te kraken is. De Duitsers werken momenteel samen met de Nijmeegse wetenschappers. Roel Verdult geeft tips over de hardware en ook op softwaregebied wordt onderling informatie uitgewisseld. TLS nog lang niet af van de kritische wetenschappers. Wordt vervolgd. x

Tekst: Alex van der Hulst